Attorney Docket No.: 15685P206 Patent Application

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

TITLE OF THE INVENTION

TIME CERTIFICATION IN A WIRELESS COMMUNICATIONS NETWORK

INVENTORS

MITHAT C. DOGAN
BRANISLAV MEANDZIJA
MARC GOLDBURG

Prepared by

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP
12400 WILSHIRE BOULEVARD
SEVENTH FLOOR
LOS ANGELES, CA 90025-1026
(408) 947-8200

EXPRESS MAIL CERTIFICATE OF MAILING

"Express Mail" mailing label number: EV330680557US
Date of Deposit: June 24, 2003
I hereby certify that I am causing this paper or fee to be deposited with the United States Postal Service "Express Mail Post Office to Addressee" service on the date indicated above and that this paper or fee has been addressed to Mail Stop Patent Application, Commissioner for Patents P.O. Box 1450 Alexandria, VA 22313-1450

Patricia M. Richard
(Typed or printed name of person mailing paper or fee)

PMRichard
(Signature of person mailing paper or fee)

6/24/2003
(Date signed)

I:\ArrayComm\P206 - i-TAP Time Certification\P206 Application.doc

Time Certification in a Wireless Communications Network

BACKGROUND OF THE INVENTION

Field of the Invention

[0001] The present invention applies to the field of hardware authentication, in particular to time certification in a wireless network.

Description of the Prior Art

[0002] Hardware authentication, also sometimes referred to as entity authentication, is the process of verifying a claimed or presumed identity. In the context of a wireless access network, hardware authentication is used to verify that a an entity is indeed the entity it is claiming to be. For example, a hardware authentication can verify that a terminal claiming to have a certain MAC address really has the claimed MAC address. Without hardware authentication, unauthorized user terminals could steal the resources of the wireless access network, and uplink and downlink communications between legitimate user terminals and access points may be intercepted and eavesdropped.

[0003] Hardware authentication in wireless networks is currently accomplished by time varying challenge-response protocols. In a typical challenge-response protocol a claimant proves its identity to a verifier by demonstrating knowledge of a secret known to be associated with the claimant.

[0004] One problem with challenge-response protocols is that the verifier needs access to a secure database to identify the secret the claimant should have. Furthermore, such protocols require several message exchanges and on-the-fly encryption that can slow down network access.

[0005] User terminals getting their sense of time from access points can cause another problem in some wireless access networks. The access point can get their time from wired networks, or the Global Positioning System. Before the terminal can authenticate the access point it may need a sense of time. However, the access point is not yet authenticated. Thus, its time reference cannot always be trusted.

BRIEF SUMMARY OF THE INVENTION

[0006] The time reference of a user terminal that is derived from an unauthenticated access point can be certified by a trusted entity according to the present invention. In one embodiment, the present invention includes a user terminal obtaining a time reference from an access point of a wireless access network. The user terminal then receives a digital certificate having a validity period from the access point, the certificate being issued by a certificate authority. In one embodiment, the user terminal requests certification of the time reference by a trusted entity, and receives the certification. Then the user terminal can validate the digital certificate.

BRIEF DESCRIPTION OF THE DRAWINGS

[0007] The present invention is illustrated by way of example, and not by way of limitation, in the figures of the accompanying drawings in which like reference numerals refer to similar elements and in which:

[0008] **Figure 1** is a simplified block diagram of a wireless access network in which one embodiment of the present invention can be practiced;

[0009] **Figure 2** is a simplified flow chart of an authentication protocol according to one embodiment of the present invention;

[0010] **Figure 3** is a simplified block diagram of a message used to authenticate a terminal according to one embodiment of the present invention;

[0011] **Figure 4** is a simplified block diagram of an access point on which an embodiment of the invention can be implemented; and

[0012] **Figure 5** is a simplified block diagram of a user terminal on which an embodiment of the invention can be implemented.

DETAILED DESCRIPTION OF THE INVENTION

In one embodiment, the UT derives its sense of time from the BS. As part of authentication, the UT can request a certified timestamp from a trusted entity such as a times server or a certificate authority.

Wireless Access Network

[0013] An example system that can be improved by using embodiments of the present invention is now described with reference to Figure 1. Figure 1 shows a wireless access network 100. The wireless access network can be used to provide access to the Internet 102, or any other data network, such as a LAN or WAN.

[0014] The wireless access network 100 includes wireless access points 104 ("AP") to allow end user devices 106 ("EUD") to communicate using wireless user terminals 108 ("UT"). An EUD 106 is generally a mobile computing device, such as a laptop or notebook computer, a personal digital assistant ("PDA"), or a cellular telephone. However, an EUD 106 can be any other computing device, such as a desktop computer or a workstation.

[0015] A UT 108 can be implemented as a stand-alone unit, such as a PCMCIA card or box, or be integrated into the body of the EUD 106. One UT 108 can provide communications for just one EUD 106 or a group of EUDs 106. The UT 108 is a communications device analogous to a modem. The UT 108 can be responsible for radio communications and physical layer signal processing. Higher lever processing can be performed by either the UT 108 or a host EUD 106.

[0016] The UT 108 communicates wirelessly, e.g. using radio signals, with an AP 104. An AP can be a cellular base station, an 802.11 access point, or other wireless system access point, such as an i-Burst™ base station. Multiple APs can be connected by a switch 110 or router to centralize the connection to the Internet 102 and to facilitate handoffs when a UT 108 moves from one AP 104 zone into another. The wireless access network 100 can be used to provide access to networks besides the Internet 102, such as Wide Area Network, Local Area Network, or the Public Switched Telephone Network.

[0017] Embodiment of the present invention need not be practiced in a strict wireless access network context. For example, one embodiment of the present invention may be in a wireless peer-to-peer network. During authentication however, one peer will be acting as an AP 104 and the other as the UT 108 of a wireless access network.

<u>Authentication Protocol</u>

[0018] An authentication protocol according to one embodiment of the present invention is shown in Figure 2. Several embodiments of the present invention are described with reference to Figure 2. Furthermore, Figure 2 also contains details not necessary to practice the present invention that are provided for clarity and context. The process and message exchange described with reference to Figure 2 is mostly related to UT 108 authentication. However, the process can also result in AP 104 authentication and the exchange of a shared secret to be used later for encryption.

[0019] When at UT 108 arrives in the coverage area of an AP 104 it begins the registration process. Registration is a relationship that enables the UT 108 to exchange communications streams with the AP 104. The authentication protocol described with reference to Figure 2 is a part of the registration process.

[0020] Since the authentication protocol described with reference to Figure 2 is certificate-based, before registration begins the UT 108 and the AP 104 are each assigned at least one digital certificate from one or more trusted entities, such as certificate authorities ("CA"). A digital certificate is a text message that is signed by the CA. The signature may be a digest of the text message encrypted with a CA private key that only the CA has access to, but that can be verified by any entity which knows the CA public key which is openly available.

[0021] To verify a certificate, one decrypts the signature with the published CA public key and computes the digest from the text message. If these two text strings match, that the certificate was indeed signed by the CA. There are commercial CAs, such as VeriSign, Inc., or a network operator can create its own CAs. Public key cryptography and its use to create and verify digital certificates is well known.

[0022] In one embodiment, the UT 108 has no independent time reference and receives its sense of time from the AP 104. For example, the AP 104 can include an absolute frame number in a broadcast burst or some communication addressed to the UT 104.

[0023] The authentication protocol can begin when the UT 104 receives the AP certificate in block 202. The AP certificate can include an identity of the AP 104, such as a media access control (MAC) address of the AP 104, which identifies the AP 104

either uniquely or network-wide. The certificate also includes the AP public key that corresponds with the private key of the AP 104. The AP 104 may use different public/private key pairs for different UTs 108. As explained above, the AP certificate is signed by a CA trusted by the UT 108.

[0024] In block 204, the UT 108 generates a shared secret. This shared secret is only known by the UT 108 at this point and will only be shared with the AP 104. The shared secret can be generated as a random sequence using a random number sequence generator. In one embodiment, at least a part of this shared secret will later be used as a master secret to encrypt communications between the UT 108 and the AP 104 using symmetric key cryptography. The necessity of establishing such a secret for symmetric key cryptography is well known.

[0025] In block 206, the UT 108 generates an authenticator string. One key purpose of the authenticator string is to demonstrate that the UT 108 is in possession of the UT private key corresponding to the UT public key contained in the UT certificate. Since the CA certifies that the public key belongs to the UT 108, any device having the corresponding private key is the authentic UT 108.

[0026] There are numerous possible authenticator strings that can demonstrate possession of the UT private key. For example, the UT can encrypt a part of the shared secret with the private key. In one embodiment, the UT 108 can generate an authenticator message and sign it with the UT private key. If the AP 104 can independently generate the authenticator message, the authenticator string can be the signature only.

[0027] In block 208, the UT 108 scrambles the UT certificate given to in by the CA. The UT certificate includes an identifier of the UT 108, such as its MAC address, and a public key associated with the private key used to sign the authenticator string. The certificate can include various other data fields containing information about the UT 108. One reason for scrambling the UT certificate is to hide the UT identifier. This makes tracking the UT 108 difficult.

[0028] In one embodiment, the UT certificate is scrambled using at least a part of the shared secret. In one embodiment, the bits of the shared secret that are used for scrambling are not reused for symmetric key cryptography later on. For example, the designated scrambling bits of the shared secret can be used to seed a linear feedback shift register whose output can be used to scramble the UT certificate. In one embodiment, the bits generated by the linear feedback shift register are XOR-ed with the bits of the UT certificate.

[0029] In block 210, the UT 108 encrypts the shared secret generated in block 204 with the AP public key contained in the AP certificate received in block 202. In one embodiment, the UT also generates a timestamp in block 212. The timestamp represents time as known by the UT 108. In one embodiment, the UT 108 derives its sense of time from the AP 104 as explained above.

[0030] In block 214, the UT 108 sends a message to the AP 104 that the AP 104 can use to authenticate the UT 108. In one embodiment, the message includes the shared secret generated in block 204 and encrypted in block 210, the UT certificate issued by the CA and scrambled in block 208, and the authenticator string generated in

block 206. Furthermore, the message can also include the timestamp generated in block 212 to protect against replay attacks.

[0031] In one embodiment, the message is a UT parameters message, which in addition to the above, also includes a variety of other information, some of which may be encrypted with the AP public key. For example, the UT parameters message can also include such parameters of the UT 108 as the communication capabilities and preferences of the UT 108.

[0032] The ordering of the blocks in Figure 2 represents merely one embodiment, and is in no way limiting. In some embodiments, several values to be included in the UT parameters message can be pre-calculated causing some blocks will this be preformed in different orders. Other blocks can be completely omitted. For example, if the UT 108 already has a trusted time reference, e.g. when the UT 108 already has the time from an authenticated AP 104, block 226 and perhaps block 212 may be omitted. Furthermore, the UT 108 may have a stored copy of the AP certificate from a prior registration. In this case block 202 may have been already performed. In one embodiment, the UT 108 stores AP certificates, or at least AP public keys, for several frequently accessed APs 104.

[0033] In one embodiment, the UT 108 generates the shared secret in block 204 before registration even begins. In other embodiments, multiple shared secrets can be generated to be used for different access points 104. In one embodiment, The UT 108 generates the shared secret, block 204, and encrypts it with several stored AP public keys stored in memory, block 210, before ever receiving the AP certificate in block 202. Furthermore, once the shared secret is generated, block 204, it can be used to

scramble the UT certificate, block 208, before registration even begins, and certainly before receiving the AP certificate in block 202. In other embodiments, the authenticator string can be generated in block 206 prior to receiving the AP certificate in block 202.

[0034] As demonstrated above, the blocks of Figure 2 that are performed by the UT 108 can be performed in various orders, and the invention is not limited to any specific event flow. Various values may be pre-calculated before registration begins, or while awaiting a protocol response from the AP 104. Furthermore, some blocks may be performed in parallel, while others may simply be switched. Pre-calculating values and speculatively encrypting the shared secret by guessing the AP identity and public key can further increase the speed and efficiency of the authentication protocol.

[0035] Referring again to Figure 2, in block 216, the AP 104 receives the UT parameters message sent by the UT 108. In block 218, the AP uses its private key to decrypt the shared secret. After the AP is in possession of the shared secret, in block 220, the AP can unscramble the UT certificate. Since at least a part of the shared secret was used in scrambling the UT certificate, only the AP 104 can unscramble it, since only the AP 104 has the AP private key necessary to decrypt the shared secret.

[0036] In block 222, the AP verifies the UT certificate by checking the CA signature and any validity period associated with the UT certificate. The UT certificate, as explained above, contains the UT public key, and the CA signature assures that this UT public key is assigned to a UT having the identifier, e.g., MAC address, also included in the UT certificate.

[0037] In block 224, the AP 104 authenticates the UT 108. This can be accomplished by using the authenticator string to verify that the UT 104 is in possession of the UT private key corresponding to the UT public key in the UT certificate. In one embodiment, the authenticator string is the UT signature over an authenticator message. The UT signature can be a digest, i.e. hash, of the authenticator message encrypted with the UT private key. Other digital signatures are also possible, such as encrypting the entire authenticator message, or a part thereof, with the UT private key.

[0038] In one embodiment, the AP 104 can generate the authenticator message and the authenticator message digest independently. In this case, the AP 104 decrypts the authenticator sting with the UT public key, generates a digest of the authenticator message, and compares the decrypted authenticator string to the independently generated authenticator message digest. In this manner, the AP 104 can verify that the UT 108 is in possession of the UT private key paired with the UT public key in the UT certificate.

[0039] In one embodiment, the UT 108 can also request time certification. In such an embodiment, the UT's 108 sense of time is derived from the AP 104 when the UT powers up. Thus, at least when a cold-start is performed but in other situations as well, an unauthorized AP could use an expired certificate and give a UT a false time reference that makes the certificate appear valid. To mitigate this problem, the UT 108 can ask the AP 108 to certify the timestamp generated by the UT 104 in block 212.

[0040] If the UT 108 requests time verification, in block 226, the AP can certify the timestamp. The timestamp can be included in the UT parameters message as a

protection against replay attacks, but it can also be used for time certification. In one embodiment, the AP 104 performs time certification in block 226 by forwarding the timestamp to a trusted time server ("TS"). The TS is trusted by the UT 108, and can be a CA, or any server known to be operated by the network operator or some other trusted entity.

[0041] In one embodiment, the TS certifies the timestamp and sends it back to the AP 104, which in turn forwards it on the UT 108. In one embodiment, in block 228, the AP 104 sends a registration parameters message to the UT 108 including various registration parameters – such as random access channels, a paging identifier, and a registration identifier – and the certified timestamp is included in this message. In other embodiments, the TS may communicate the certification directly to the UT 108, or by some other means besides the AP 104.

[0042] According to one embodiment described with reference to Figure 2, the AP 104 can authenticate the UT 108 using a single message from the UT 108. In one embodiment, all further communication between the UT 108 and the AP 104 is encrypted using the shared secret, or a part of it, for symmetric cryptography. In this case, when the AP 104 sends the registration message in block 228, the AP 104 is implicitly authenticated, since only the AP possessing the AP private key has the shared secret outside of the UT 108.

[0043] As mentioned above, the UT parameters message, discussed above is enough for the AP 104 to authenticate the UT 108. Figure 3 further demonstrates some aspects of the UT parameters message in accordance with a specific embodiment of the invention. As Figure 3 illustrates, the UT parameters message 302 used to authenticate

the UT 108 can have other fields. The message fields discussed with reference to Figure 3 are message fields 302A, 302B, and 302C.

[0044] As described above, field 302A is generated by scrambling 304 the UT certificate 306. As shown by dotted line 308, a part 310A of the shared secret 310 is used for the scrambling 304. Secret 310A is used to initialize a linear feedback shift register. Then, the LFSR's output is XOR-ed with the UT certificate 306. This hides the UTID 312 from eavesdroppers, and makes UT tracking more difficult. To unscramble the UT certificate 306 an AP will need to know the shared secret 310.

[0045] Field 302B contains the shared secret 310 encrypted 320 with the AP public key. Since only the AP who possesses the private key corresponding with this public key can decrypt the shared secret 310, only this AP can unscramble the UT certificate.

[0046] Field 302C contains the authenticator string that proves possession of the UT private key. Generally, proof of a private key is demonstrated by sending a message signed with the private key. For efficiency, most digital signatures first generate a digest of the message and encrypt the digest with the private key.

[0047] Field 302C is generated by creating an authenticator message 314 including the UTID 312, i.e. MAC address, copied from the UT certificate 306 (as demonstrated by dotted line 316), a copy of the shared secret 310 (as demonstrated by line 318), and the absolute frame number of the frame when the UT parameters message 302 is to be sent. In one embodiment, the absolute frame number is a 48-bit number representing the number of 200Hz periods since the beginning of the Global Positioning System GPS epoch. The absolute frame number is the primary time parameter for the UT in one embodiment. The authenticator message 314 thusly generated is unique, different

with every registration, includes a temporal element – the absolute frame number – to protect against replay attacks, combines copied elements from other fields, and can be independently regenerated by the AP provided that the AP can decrypt the shared secret.

[0048] As explained above, the authenticator message is signed 328 by first generating a digest 322 of the authenticator message 314. The digest can be generated by a one-way hash function. The authenticator message digest is then encrypted 236 with the UT private key to produce the UT signature that is inserted into field 302C.

[0049] Since the AP can generate the authenticator message 314 independently and knows the hash function, the AP can verify possession of the UT private key by decrypting the received authenticator string in field 302C with the UT public key included in the UT certificate 306, and comparing the result with the independently generated authenticator message digest.

[0050] As mentioned with reference to Figure 2, fields 302A, 302B, and 302C can be pre-computed. The shared secret 310 – which is a random sequence – can be generated at any time. Field 302A can thus be generated at any time, although scrambling does not require intensive computing and can also be performed in real time.

[0051] To generate field 302B, the AP public key must be known. A UT can store the public keys of some APs that the UT frequently communicates with. If the UT encrypts 320 the shared secret with all the public keys stored by the UT, when the AP is identified, no more encryption is necessary; the appropriate encrypted version of the shared secret can be inserted for field 302B. In this manner, the UT can speculatively

pre-calculate field 302B before even receiving the AP certificate. When the AP certificate is received, the UT need only verify that the public key stored for the particular AP is still valid.

[0052] Field 302C can also be speculatively pre-calculated. After registration has begun, the UT can guess at the absolute frame number in which the UT parameters message 302 will be transmitted. The other elements of the authenticator message 312 are known. Thus, after guessing one or more absolute frame numbers, one or more possible authenticator messages can be generated, and each encrypted 326 with the UT private key. When the UT parameters message's 302 absolute frame number is known, the correct one can be inserted into field 302C. If all guesses were wrong, a new authenticator string could be calculated without losing any time, since without guessing, the generation could not have yet begun.

Access Point Structure

[0053] Embodiments of an AP 104 and a UT 108 of a wireless access network are now described. Figure 4 shows an example of an AP of a wireless access network or cellular communication network suitable for implementing the present invention. The system or network includes a number of subscriber stations, also referred to as remote terminals or UTs, such as that shown in Figure 1 as UT 108 and in detail in Figure 5. The AP may be connected to a wide area network (WAN) or the Internet through its host DSP 31 for providing any required data services and connections external to the immediate wireless system. To support spatial diversity, a plurality of antennas 3 is used, for example four antennas, although other numbers of antennas may be selected.

[0054] A set of spatial multiplexing weights for each subscriber station are applied to the respective modulated signals to produce spatially multiplexed signals to be transmitted by the bank of four antennas. The host DSP 31 produces and maintains spatial signatures for each subscriber station for each conventional channel and calculates spatial multiplexing and demultiplexing weights using received signal measurements. In this manner, the signals from the current active subscriber stations, some of which may be active on the same conventional channel, are separated and interference and noise suppressed. When communicating from the AP to the subscriber stations, an optimized multi-lobe antenna radiation pattern tailored to the current active subscriber station connections and interference situation is created. Suitable smart antenna technologies for achieving such a spatially directed beam are described, for example, in U.S. Patents Nos. 5,828,658, issued Oct. 27, 1998 to Ottersten et al. and 5,642,353, issued June 24, 1997 to Roy, III et al. The channels used may be partitioned in any manner. In one embodiment the channels used may be partitioned as defined in the GSM (Global System for Mobile Communications) air interface, or any other time division air interface protocol, such as Digital Cellular, PCS (Personal Communication System), PHS (Personal Handyphone System) or WLL (Wireless Local Loop). Alternatively, continuous analog or CDMA channels can be used.

[0055] The outputs of the antennas are connected to a duplexer switch 7, which in a TDD embodiment, may be a time switch. Two possible implementations of the duplexer switch are as a frequency duplexer in a frequency division duplex (FDD) system, and as a time switch in a time division duplex (TDD) system. When receiving, the antenna outputs are connected via the duplexer switch to a receiver 5, and are

converted down in analog by RF receiver ("RX") modules 5 from the carrier frequency to an FM intermediate frequency ("IF"). This signal then is digitized (sampled) by analog to digital converters ("ADCs") 9. Final down-converting to baseband is carried out digitally. Digital filters can be used to implement the down-converting and the digital filtering, the latter using finite impulse response (FIR) filtering techniques. This is shown as block 13. The invention can be adapted to suit a wide variety of RF and IF carrier frequencies and bands.

[0056] There are, in the present example, eight down-converted outputs from each antenna's digital filter 13, one per receive timeslot. The particular number of timeslots can be varied to suit network needs. While GSM uses eight uplink and eight downlink timeslots for each TDMA frame, desirable results can also be achieved with any number of TDMA timeslots for the uplink and downlink in each frame. For each of the eight receive timeslots, the four down-converted outputs from the four antennas are fed to a digital signal processor (DSP) 17 (hereinafter "timeslot processor") for further processing, including calibration, according to one aspect of this invention. Eight Motorola DSP56300 Family DSPs can be used as timeslot processors, one per receive timeslot. The timeslot processors 17 monitor the received signal power and estimate the frequency offset and time alignment. They also determine smart antenna weights for each antenna element. These are used in the SDMA scheme to determine a signal from a particular remote user and to demodulate the determined signal.

[0057] The output of the timeslot processors 17 is demodulated burst data for each of the eight receive timeslots. This data is sent to the host DSP processor 31 whose main function is to control all elements of the system and interface with the higher

level processing, which is the processing which deals with what signals are required for communications in all the different control and service communication channels defined in the system's communication protocol. The host DSP 31 can be a Motorola DSP56300 Family DSP. In addition, timeslot processors send the determined receive weights for each UT to the host DSP 31. The host DSP 31 maintains state and timing information, receives uplink burst data from the timeslot processors 17, and programs the timeslot processors 17. In addition it decrypts, descrambles, checks error correcting code, and deconstructs bursts of the uplink signals, then formats the uplink signals to be sent for higher level processing in other parts of the AP. Furthermore DSP 31 may include a memory element to store data, instructions, or hopping functions or sequences. Alternatively, the AP may have a separate memory element or have access to an auxiliary memory element. With respect to the other parts of the AP it formats service data and traffic data for further higher processing in the AP, receives downlink messages and traffic data from the other parts of the AP, processes the downlink bursts and formats and sends the downlink bursts to a transmit controller/modulator, shown as 37. The host DSP also manages programming of other components of the AP including the transmit controller/modulator 37 and the RF timing controller shown as 33.

[0058] The RF timing controller 33 interfaces with the RF system, shown as block 45 and also produces a number of timing signals that are used by both the RF system and the modem. The RF controller 33 reads and transmits power monitoring and control values, controls the duplexer 7 and receives timing parameters and other settings for each burst from the host DSP 31.

[0059] The transmit controller/modulator 37, receives transmit data from the host DSP 31. The transmit controller uses this data to produce analog IF outputs which are sent to the RF transmitter (TX) modules 35. Specifically, the received data bits are converted into a complex modulated signal, up-converted to an IF frequency, sampled, multiplied by transmit weights obtained from host DSP 31, and converted via digital to analog converters ("DACs") which are part of transmit controller/modulator 37 to analog transmit waveforms. The analog waveforms are sent to the transmit modules 35. The transmit modules 35 up-convert the signals to the transmission frequency and amplify the signals. The amplified transmission signal outputs are sent to antennas 3 via the duplexer/time switch 7.

User Terminal Structure

[0060] Figure 5 depicts an example component arrangement in a UT that provides data or voice communication. The user terminal's antenna 45 is connected to a duplexer 46 to permit the antenna 45 to be used for both transmission and reception. The antenna can be omni-directional or directional. For optimal performance, the antenna can be made up of multiple elements and employ spatial processing as discussed above for the AP. In an alternate embodiment, separate receive and transmit antennas are used eliminating the need for the duplexer 46. In another alternate embodiment, where time division duplexing is used, a transmit/receive (TR) switch can be used instead of a duplexer as is well known in the art. The duplexer output 47 serves as input to a receiver 48. The receiver 48 produces a down-converted signal 49,

which is the input to a demodulator 51. A demodulated received sound or voice signal 67 is input to a speaker 66.

[0061] The user terminal has a corresponding transmit chain in which data or voice to be transmitted is modulated in a modulator 57. The modulated signal to be transmitted 59, output by the modulator 57, is up-converted and amplified by a transmitter 60, producing a transmitter output signal 61. The transmitter output 61 is then input to the duplexer 46 for transmission by the antenna 45.

[0062] The demodulated received data 52 is supplied to a user terminal central processing unit 68 (CPU) as is received data before demodulation 50. The user terminal CPU 68 can be implemented with a standard DSP (digital signal processor) device such as a Motorola series 56300 Family DSP. This DSP can also perform the functions of the demodulator 51 and the modulator 57. The user terminal CPU 68 controls the receiver through line 63, the transmitter through line 62, the demodulator through line 52 and the modulator through line 58. It also communicates with a keyboard 53 through line 54 and a display 56 through line 55. A microphone 64 and speaker 66 are connected through the modulator 57 and the demodulator 51 through lines 65 and 66, respectively for a voice communications user terminal. In another embodiment, the microphone and speaker are also in direct communication with the CPU to provide voice or data communications. Furthermore user terminal CPU 68 may also include a memory element to store data, instructions, and hopping functions or sequences. Alternatively, the user terminal may have a separate memory element or have access to an auxiliary memory element.

[0063] In one embodiment, the speaker 66, and the microphone 64 are replaced or augmented by digital interfaces well-known in the art that allow data to be transmitted to and from an external data processing device (for example, a computer). In one embodiment, the user terminal's CPU is coupled to a standard digital interface such as a PCMCIA interface to an external computer and the display, keyboard, microphone and speaker are a part of the external computer. The user terminal's CPU 68 communicates with these components through the digital interface and the external computer's controller. For data only communications, the microphone and speaker can be deleted. For voice only communications, the keyboard and display can be deleted.

General Matters

[0064] In the description above, for the purposes of explanation, numerous specific details are set forth in order to provide a thorough understanding of the present invention. It will be apparent, however, to one skilled in the art that the present invention may be practiced without some of these specific details. In other instances, well-known structures and devices are shown in block diagram form.

[0065] The present invention includes various steps. The steps of the present invention may be performed by hardware components, such as those shown in Figures 4 and 5, or may be embodied in machine-executable instructions, which may be used to cause a general-purpose or special-purpose processor or logic circuits programmed with the instructions to perform the steps. Alternatively, the steps may be performed by a combination of hardware and software. The steps have been described as being performed by either the AP or the UT. However, many of the steps described as being

performed by the AP may be performed by the UT and vice versa. Furthermore, the invention is equally applicable to systems in which terminals communicate with each other without either one being designated as a AP, a UT, a user terminal or a subscriber station. Thus, the present invention is equally applicable and useful in a peer-to-peer wireless network of communications devices. In such a network, during the execution of the authentication protocol the devices would take turns acting in the manner of the UT and the AP described above. These devices may be cellular phones, PDA's, laptop computers, or any other wireless devices. Generally, since both the APs and the UTs use radio waves, they are sometimes referred to as radios.

[0066] In portions of the description above, only the AP is described as performing spatial processing using an antenna array. However, the UTs can also contain antenna arrays, and can also perform spatial processing both on receiving and transmitting (uplink and downlink) within the scope of the present invention.

[0067] Embodiments of the present invention may be provided as a computer program product, which may include a machine-readable medium having stored thereon instructions, which may be used to program a computer (or other electronic devices) to perform a process according to the present invention. The machine-readable medium may include, but is not limited to, floppy diskettes, optical disks, CD-ROMs, and magneto-optical disks, ROMs, RAMs, EPROMs, EEPROMs, magnet or optical cards, flash memory, or other type of media / machine-readable medium suitable for storing electronic instructions. Moreover, the present invention may also be downloaded as a computer program product, wherein the program may be transferred from a remote computer to a requesting computer by way of data signals

embodied in a carrier wave or other propagation medium via a communication link (e.g., a modem or network connection).

[0068] Many of the methods and calculations are described in their most basic form, but steps can be added to or deleted from any of the methods and information can be added or subtracted from any of the described message signals without departing from the basic scope of the present invention. It will be apparent to those skilled in the art that many further modifications and adaptations can be made. The particular embodiments are not provided to limit the invention but to illustrate it. The scope of the present invention is not to be determined by the specific examples provided above but only by the claims below.

[0069] It should also be appreciated that reference throughout this specification to "one embodiment" or "an embodiment" means that a particular feature may be included in the practice of the invention. Similarly, it should be appreciated that in the foregoing description of exemplary embodiments of the invention, various features of the invention are sometimes grouped together in a single embodiment, figure, or description thereof for the purpose of streamlining the disclosure and aiding in the understanding of one or more of the various inventive aspects. This method of disclosure, however, is not to be interpreted as reflecting an intention that the claimed invention requires more features than are expressly recited in each claim. Rather, as the following claims reflect, inventive aspects lie in less than all features of a single foregoing disclosed embodiment. Thus, the claims following the Detailed Description are hereby expressly incorporated into this Detailed Description, with each claim standing on its own as a separate embodiment of this invention.